



Alkhamis, E., and Renaud, K. (2016) The Design and Evaluation of an Interactive Social Engineering Training Programme. In: International Symposium on Human Aspects of Information Security and Assurance (HAISA 2016), Frankfurt, Germany, 19 - 21 July 2016, pp. 125-134. ISBN 9781841024134.

There may be differences between this version and the published version. You are advised to consult the publisher's version if you wish to cite from it.

<http://eprints.gla.ac.uk/120717/>

Deposited on: 7 July 2016

Enlighten – Research publications by members of the University of Glasgow
<http://eprints.gla.ac.uk>

The Design and Evaluation of an Interactive Social Engineering Training Programme

Esra Alkhamis¹ and Karen Renaud²

¹King Saud University, Riyadh, Saudi Arabia
e-mail: ealkhamis@ksu.edu.sa

²University of Glasgow, Glasgow, United Kingdom
e-mail: karen.renaud@glasgow.ac.uk

Abstract

Social engineering is a major issue affecting organisational security. Educating employees on how to avoid social engineering attacks is important because social engineering tries to penetrate an organisation by using employees to grant authorized access to sensitive information. While there are a number of theoretical studies about social engineering, a few practical studies have moved towards educating and training employees on how to spot such attacks. In this research, we emphasise the importance of educating employees to make them more resilient to these kinds of attacks.

We developed an educational video encapsulated within a *Social Engineering Training Programme*. This is essentially an interactive training video during which the learner interacts with three different scenarios; educational content, a knowledge-check, and a web page containing the latest news about current social engineering attacks.

The training programme was evaluated in a Saudi trading company with 24 employees. The evaluation showed that the programme delivered a positive impact in terms of awareness, as tested by a post-training quiz.

Keywords

Social Engineering Training Programme, Security Awareness.

1. Introduction

Organisations are increasingly aware of the need for technological security measures to be deployed in order to protect their infrastructure and data. These measures are designed to ensure that unauthorised users are prevented from gaining access to company information via their networked computer systems, or from being able to gain administrative privileges to do real damage. Despite the deployment of many technological tools, data breaches still occur because employees are deceived by social engineering attacks. Social engineering is a way of manipulating people to illegally gain access to sensitive information or valuable services. Due to the natural human tendency to place confidence in others, victims willingly disclose company information. The information may seem innocuous but, when aggregated, can help to resource a more significant social engineering attack.

Social engineering is a significant threat to the security of an organisation. Teaching employees to recognise social engineering attacks is challenging because of the range of techniques used by the social engineer to deceive. Experts argue that humans are the most vulnerable elements of any security system (Hadnagy, 2011; Mitnick and Simon, 2002). Social engineering takes advantage of people's natural tendencies in order to manipulate them into disclosing information or carrying out a particular action. The problem is that employees are often unaware of this type of attack, and they underestimate the value of seemingly unimportant information in pre-empting a successful attack. Such attacks can result in negative economic and social consequences (Hadnagy, 2011).

Many organisations formulate and publish security policies to ameliorate the threat. The problem is that employees do not necessarily read or understand organisational policies, nor do they particularly realise how to apply the principles in practice. We argue here that employees need to be engaged in the teaching process in order to raise awareness of different threats (Tims, 2001). Hiner argues that education enables employees to identify concerning events that may occur which could be part of a social engineering attack. The desire is that they would report the event, and any educational endeavour should explain how to do this (Hiner, 2002).

The research reported here aimed to mitigate the social engineering risk by developing an interactive training programme to help users to understand social engineering techniques and to ensure they have the knowledge to spot and resist them.

2. Related Work

2.1. Detecting social engineering

Researchers from the University of Pretoria in South Africa proposed a model called the Social Engineering Attack Detection Model (SEADM) (Hadnagy, 2011). This model was intended to help call-centre employees identify social engineering callers. The authors use a decision tree that breaks the process down into smaller components and offers guidelines to aid employees in making a decision about how to act. This model makes a valuable contribution in terms of countering social engineering, as there is not much practical research in this field. However, even if this model aids employees in detecting social engineering attacks, it has not yet been implemented, so we cannot judge the effectiveness of the model without evaluation. Moreover, this model depends only on human reasoning to make judgments, which is not the only aspect that informs behaviour. If the victim is being subjected to intimidation or temptation, he/she will be under the kind of pressure that invalidates human reason, and can result in unwise decisions.

Researchers from Bradford University in the United Kingdom suggest detecting social engineering attacks using neural networks. This method uses benchmark data and develops a feature extraction technique to use with neural networks while testing and training. The benchmark consists of 20 conversation scenarios and nine social engineering attacks. In all of these scenarios, the employee follows the company's

call policy by asking the caller for his name, company, and job title. They filter the keywords that may indicate a social engineering attack, such as *install*, by using a feature-extraction process. These keywords are then represented in numerical training vectors to use in neural network learning, in order to carry out learning experiments that investigate the feasibility of the approach in improving identification of social engineering attacks (Sandouka *et al.* 2009). This method also makes a valuable contribution to the social engineering resistance field, and may help companies detect social engineering attacks in real life. However, the researchers did not use real-life data, and the neural network system has not yet been integrated into an existing call centre, so it is difficult to judge the detection rate of social engineering attacks.

2.2. Social engineering Training Videos

Awareness training, in the form of videos, is popular in security. However, there few videos specifically address the social engineering threat and no scientific studies related to their effectiveness in this context could be found. Many videos use text, image, and audio, but do not support interaction. The most well known is a set of training videos called *Social Engineering Awareness Training* produced by SANS Security, the world's leading provider of information security. This presentation introduces social engineering, explains how social engineering attacks are conducted, gives examples of common social engineering attacks including technical and non-technical attacks, and finally explains how to resist such attacks. The SANS training video presents essential information about social engineering attacks. The video is available in many different languages including English, Arabic and Russian.

As training videos go, this a typical approach: there is no interaction with the learner. Moreover, no texts are provided to help the learner to follow the tutor in the video. The learner might need to replay the video repeatedly to hear or understand parts of it. In the worst case, if the learner is deaf or hard of hearing, he/she will not gain any insights from this kind of training video. Finally, there is no post-video quiz or self assessment to assess the learner's understanding of the presented concepts. Without a measurement tool it is impossible to determine the efficacy of any educational intervention.

A YouTube search reveals other videos, such as *Anti Social Engineering Training Video* (1312 views) and *Social Engineering-Security Awareness* (174 views) produced by UMass Boston, but they similar in terms of their characteristics. However, the *SANS Social Engineering Awareness Training Video* seems to have the most credibility since it was produced by SANS (7037 views). [Views recorded in March 2016]

2.3. The Effectiveness of Interactive Videos in the Education and Training

Interactive videos seem to be the way forward for social engineering training. Briggs *et al.* (2006) present the following arguments for their effectiveness of interactive videos in education:

1. It can be considered one of the fastest-moving trends, as it integrates learning content, tools, and some types of service into one solution. This will enable organisations to deliver the information to the learner in a fast, effective, and economic way. The latter is also raised by Slee (1989).
2. It helps enhance learner engagement, as well as improve effectiveness, since it presents the material in a variety of ways. The effectiveness was confirmed by Zhang *et al.* (2006), who also observed a higher level of learner satisfaction.
3. It gives the learner the flexibility to manage access to the material, as they can skip some segments and replay others. This puts them into control and allows them to discover things for themselves. The desirability of this feature was also highlighted by Bosco (1986) in his review of interactive videos in education.

There is also evidence that interactive videos help learners to think more critically (Hilgenberg and Tolone, 2000) and that interaction with this kind of learning experience proved a motivating and successful experience (Watts, 1989)

3. Design of Interactive Social Engineering Training Video

Experts in educational multimedia argue that an educational process will produce an effective result when it is interactive, motivating, and has plenty of action (Stemler, 1997). The training programme we present here has four characteristics that make it likely to be effective, relevant and more motivational than the available training tools: (1) Scenario-based, (2) Own-Pace Learning, (3) Interactive, and (4) Accessibility (Disability-support).

The objective of developing the training program was to educate employees in detecting and resisting social engineering attacks. The idea was to impart knowledge of the techniques commonly used by social engineers. We also wanted to assist employees in making decisions regarding different scenarios that could occur in organisations, as well as the advised actions to take.

Learners' interactions with the programme is in the form of posed knowledge-check sections and being able to view the latest news about current social engineering attacks. Regarding motivation, if the training program is designed for a specific organisation this means employees ought to be more motivated to follow the security policies since they are more likely to understand what is expected.

The *Social Engineering Training Program* consists of three main parts as shown in Figure 1: educational content about social engineering, a knowledge-check section, and a social engineering latest news page.

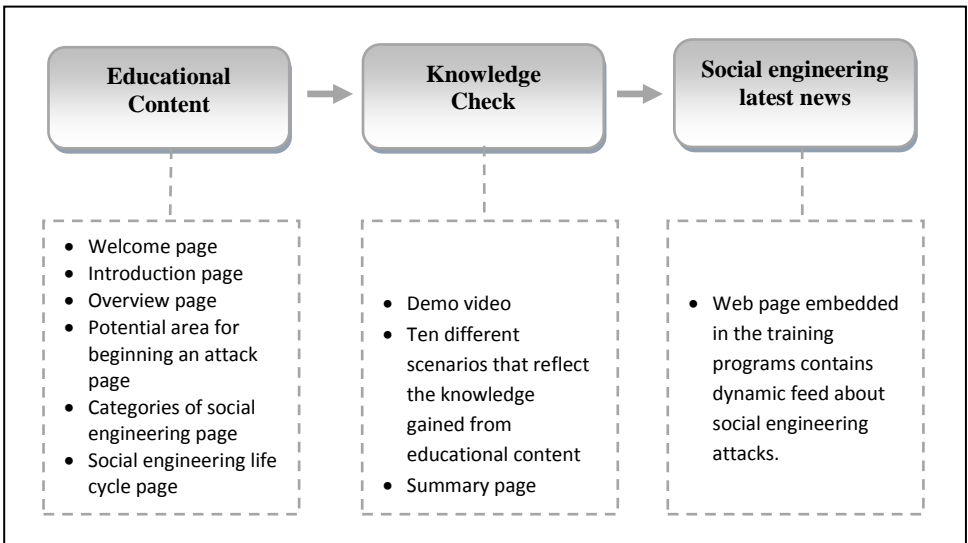


Figure 1: Social Engineering Training Program

3.1. Implementing the educational content pages

Figure 2 depicts the *Social Engineering Training Program* introduction page. Here the learner has the flexibility to control their progression through the training program by means of the use of a playback player at the end of the page that allows rewind, play, go back, go forward or open/close the closed caption.



Figure 2: Introduction page

In Figure 3 the human- and computer-facilitated attacks for each attack category are displayed. As the training program is learner-driven, the learner can mouse-over each type of attack to explore each type (see Figure 4).

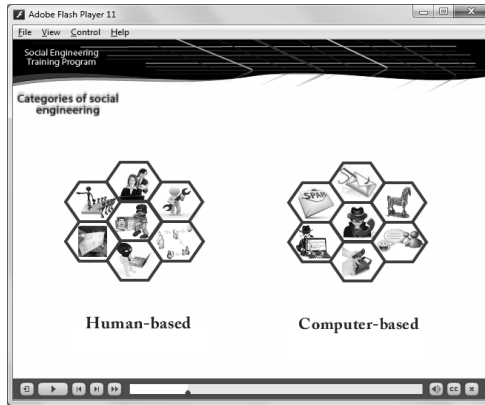


Figure 3: Categories of social engineering page

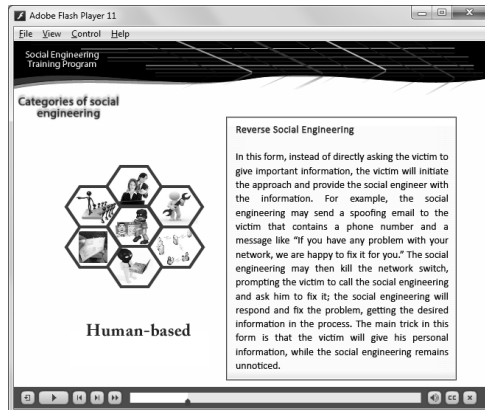


Figure 4: Categories of social engineering page (Rollover feature)

3.2. Implementing the Knowledge-Check Content

On the knowledge-check page, a demo video illustrates how to interact with this section. Moreover, for each scenario there are two main pages, and three different messages. The first is the scenario page, which presents a common workplace scenario (Figure 5). The second is the challenge page (Figure 6), which offers different options. The learner then makes a choice. The system responds based on the correctness of the choice. If the answer is correct a green box appears containing the text *“Correct. You should”* if wrong, a red box appears containing *“Be careful! You should not”* In both situations he/she can optionally click on an information button to learn more (Figure 7). The learner can also skip any question if he/she prefers.



Figure 5: Scenario page



Figure 6: Answer page

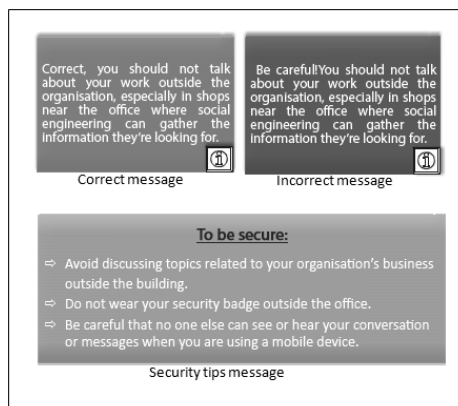


Figure 7: Answer page messages

After the learner completes the entire scenario he/she can go back and view the correct answer for the scenarios.

3.3. Implementing the Social Engineering Latest News page

When the learner clicks on the check news button a new browser window will open containing up-to-date news about current social engineering attacks.

4. Evaluation of the Social Engineering Training Program

4.1. Participants

As this training program was aimed specifically at the organisational sector, we evaluated it with employees in a small organisation. The Saudi company where the programme was evaluated is a trading company with 24 employees with a range of ages, genders and educational backgrounds.

4.2. Procedure

Pre- and post-test questionnaires were developed to measure the effectiveness of the *Social Engineering Training Program* to test the research hypothesis “*Interactive training video are feasible, effective tools for training and educating people on how to avoid social engineering attacks*”. Questionnaires were completed online before and after the video was viewed. 11 males and 13 females participated, first completing the pre-test questionnaire, then interacting with the *Social Engineering Training Program*, then completing the post-test questionnaire.

4.3. Analysis

Only seven participants had prior knowledge of social engineering attacks. The majority of these had heard about social engineering but were not able to provide many details. Three of the seven knew how to avoid attacks but had not previously experienced such an attack.

When the employees were asked about the best way to raise the awareness of social engineering the majority believed that training programmes would be the best method. Other methods mentioned were newspaper articles and security brochures. All considered an interactive training video to be an effective educational tool.

The majority of respondents had received emails and phone calls from an unknown person trying to get their sensitive information. However, when we asked employees about social engineering they did not link that concept to these emails and calls.

Figure 8 shows that the employees had a greater understanding of social engineering and of the techniques involved *after* interacting with the *Social Engineering Training Program*. They demonstrated a knowledge gain and were able to apply most of their new knowledge correctly in the post-test questionnaire. 79% of their answers were

correct with 151/192 correct answers in the post-test questionnaire. Only 36% of their answers were correct (70/192) in the pre-test questionnaire. These results demonstrate the benefits of the interactive training video in the educational field.

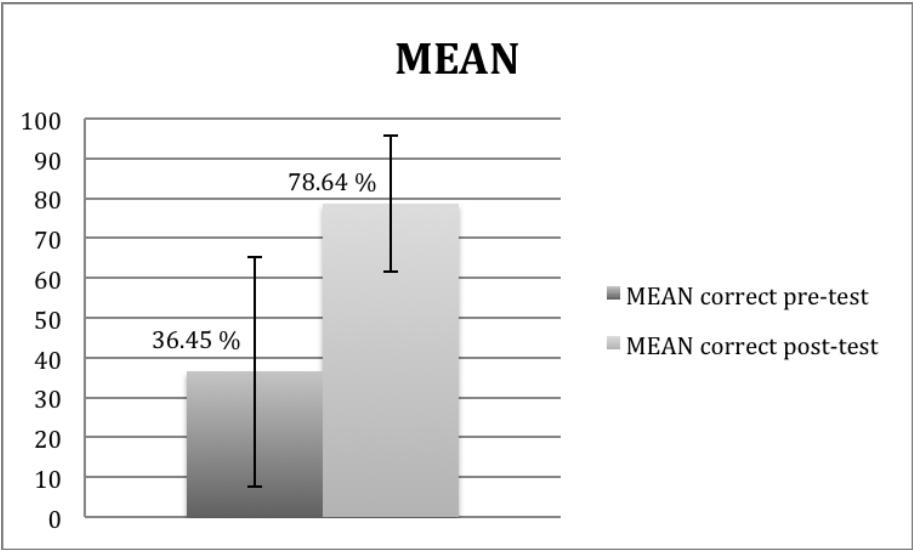


Figure 8: Overall correct answers for pre and post test questionnaire

4.4. Statistical Evaluation

In order to give more strength to the findings we carried out a statistical evaluation of the differences between the pre- and post-quizzes. The t-test is a statistical analysis function used to determine whether the knowledge improvement effects were statistically significant or not. To apply the t-test we compared the correct results for each employee before and after interacting with the training program. The p-value was 0.000000242, which exhibits a highly significant result.

5. Conclusion

The initial objective for this research was to implement and measure an effective interactive training programme to help people to resist social engineering attacks. The implemented product (*Social Engineering Training Programme*) demonstrated its promise in an organisational setting evaluation. It should clearly be tested in other organisations too to ensure that the initial promise is confirmed.

6. References

Allen, M. (2006). Social Engineering: A means to violate a computer system. Available from: http://www.sans.org/reading_room/whitepapers/engineering/social-engineering-means-violate-computer-system_529 [accessed 17 March 2016].SANS Institute.

Bezuidenhout, M., Mouton, F. and Venter, H.S. (2010). Social engineering attack detection model: SEADM. *Information Security for South Africa VN*, 1-8.

Bosco, J. (1986). An analysis of evaluations of interactive video. *Educational Technology*, 26(5), 7-17.

Briggs, R. , Nunamaker, J, Zhang, D., and Zhou, L.. (2006). Instructional video in e-learning: assessing the impact of interactive video on learning effectiveness. *Inf. Manage.* 43, 1.

Hadnagy, C. (2011). *Social engineering: The art of human hacking*. Indianapolis: Wiley Publishing, Inc.

Hilgenberg, C., & Tolone, W. (2000). Student perceptions of satisfaction and opportunities for critical thinking in distance education by interactive video. *American Journal of Distance Education*, 14(3), 59-73.

Hiner, J. (2002). Change your company's culture to combat social engineering attacks. Tech Republic [online]. Available from: <http://www.techrepublic.com/article/change-your-companys-culture-to-combat-social-engineering-attacks/1047991> [accessed 17 March 2016].

Hunt, T. (2012). Scamming the scammers – catching the virus call centre scammers red-handed. Available from: <http://www.troyhunt.com/2012/02/scamming-scammers-catching-virus-call.html#more> [accessed 1 March 2016].

Mahmood, A., Pahnla, S. and Siponen, M. (2007). Employees' behaviour towards IS security policy compliance. *System Sciences VN*, 156b.

Mitnick, K.D. and Simon, W.L. (2002). *The art of deception*. Indianapolis: Wiley Publishing, Inc.

Sandouka, H., Cullen, A.J. and Mann, I. (2009). Social engineering detection using neural networks. *CyberWorlds VN*, 273-278.

SANS Institute. Aweraness training demo. [Video] Available at: <http://www.securingthehuman.org/services/awareness-videos/social-engineering/> [accessed 14 August 2015].

Slee, E. J. (1989). A Review of the Research on Interactive Video. Proceedings of Selected Research Papers presented at the Annual Meeting of the Association for Educational Communications and Technology (Dallas, TX, February 1-5, 1989).

Stemler, L.(1997). Educational characteristics of multimedia: a literature review. *J. Educ. Multimedia Hypermedia* 6, 3-4 (October 1997), 339-359.

Tims, R. (2001). Social engineering: Policies and education a must. SANS Institute.

Watts, C. (1989). Interactive video: what the students say. *Calico Journal*, 17-20.

Zhang, D., Zhou, L., Briggs, R. O., & Nunamaker, J. F. (2006). Instructional video in e-learning: Assessing the impact of interactive video on learning effectiveness. *Information & management*, 43(1), 15-27.